V-OS APP IDENTITY

Establishing A Digital Trust Ecosystem

A Holistic Zero Trust Strategy Needs App Identity

The central concept of a Zero Trust Strategy is "never trust, always verify". But how do you establish trust between different mobile applications? As mobile apps evolve to become more complex and collaborative, there is an increasing need for apps to communicate with one another (and with other systems) to have some means to establish mutual trust. This is especially relevant for applications that depend on other apps for user authentication, payment, and securely transferring data for trusted storage or processing.

To ensure an app's identity and integrity and to establish a trusted communication channel between apps and endpoints, V-Key's V-OS App Identity solution creates an app-based software secure element that is bound to every relevant app. With this app-based secure element, trust can easily be established and verified, whether between an app communicating with another app on the same device, or across different devices. This can even be taken further to create a trusted communication channel between server applications.

Ensuring Mutual Trust Between Apps

App-to-app mutual trust can occur in many different combinations. Depending on the actual use case, some of these combinations may require only one app to trust another but not vice-versa ("One-sided trust" -- e.g. when an app needs to verify a user's identity through a mobile authenticator). There are also use cases where both apps need to mutually trust each other ("mutual trust" – e.g when a shopping app needs to send confidential data to a payment app).

Product Features

- MULTI LAYERED SECURITY FOR CRYPTO KEYS PROTECTION
- APP RUN-TIME TAMPERING PROTECTION
- MITM ATTACK PREVENTION FOR DATA-IN-TRANSIT
- PROTECTION OF CLOUD API CALLS FROM SPOOFING ATTACKS
- STRONGER PUBLIC KEY CRYPTOGRAPHY USING RSA/SHA256
- SIGNING AND DECRYPTION USING UNIQUE APP PRIVATE KEY

WHAT WE DO

V-Key is a software-based digital security company whose technology powers security solutions that deliver the highest level of defence and control for digital identity, user authentication, access and authorisation -- without compromising the user experience. It is trusted by government, banking, and mega-app clients across the region to connect people, organisations, and devices everywhere by securing the global digital economy.

OUR MISSION

To provide a secure Universal Digital Identity to power trusted digital services globally.

V-Key provides trusted, reliable, and secure Digital ID services that enable people to truly and safely participate in the modern economy.

SCAN FOR MORE INFO ON APP ID:

Contact insidesales@v-key.com

V-OS VIRTUAL SECURE ELEMENT • V-OS APP IDENTITY
V-OS MOBILE APP PROTECTION • V-OS MOBILE SMART TOKEN • V-KEY SMART AUTHENTICATOR

info@v-key.com www.v-key.com

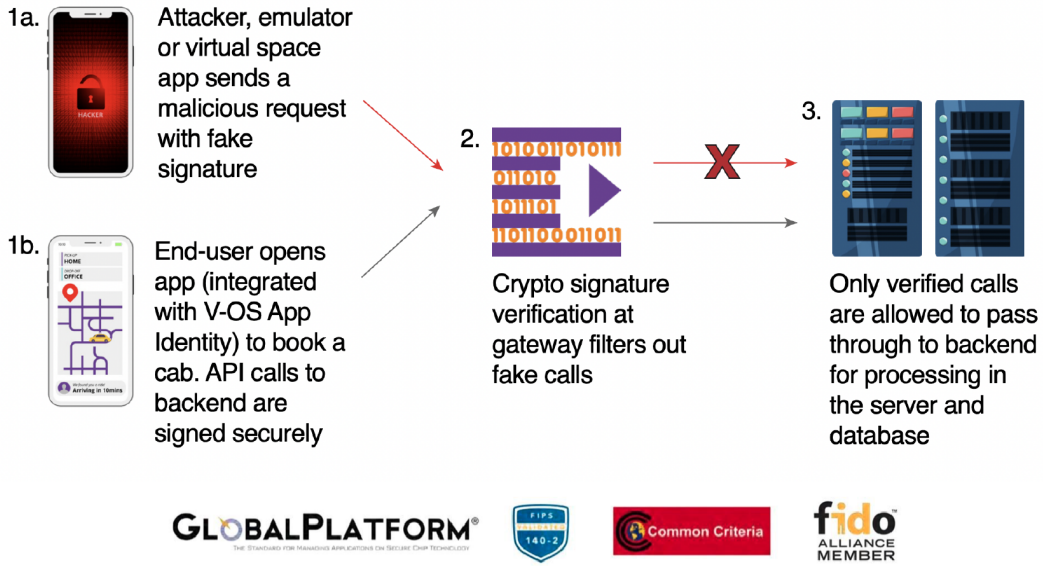
Zero Trust and The Trust Gap Issue

V-Key's research team has released a white paper detailing a general architectural design that hackers can exploit to get an app's authenticator keys or other important cryptographic elements, even if the phone's Trusted Execution Environment (TEE) is used. When mobile authenticators are targeted, hackers can make unauthorised transactions or sign bogus documents, regardless of any hardware-based protection provided by a phone. This is especially true for jailbroken phones, rooted devices, or models susceptible to what is known as a "privilege escalation vulnerability." The targeted app doesn't even need to be running or be tampered with to be compromised. V-Key calls this very serious design flaw the **Trust Gap.**

Security architectures that seem to be very secure in the past are no longer safe. Most cybersecurity practitioners have generally assumed that as long as an app can make use of a secure element or TEE for critical operations, it would be protected. But the Trust Gap attack shows that this can no longer be taken for granted, as both the app and TEE must be treated as separate endpoints that require mutual verification of trust.

This is a critical gap in the Zero Trust approach -- it should require every endpoint, whether it be a server, a device, or an individual app to be able to verify its own integrity and authenticate itself to other endpoints in the network. This includes protecting even APIs in the cloud. Only V-OS App Identity can provide a secure element bound to every app (and end point) which can serve as proof of identity and integrity without the need for any external authenticators -- but also without compromising the user experience.

Providing Cloud API Protection with V-OS App Identity



GLOBALPLATFORM · FIPS 140-2 · Common Criteria · fido ALLIANCE MEMBER

TO DOWNLOAD THE TRUST GAP WHITE PAPER. SCAN HERE:

THE TRUST GAP ISSUE AS FEATURED ON CNN'S THE FINAL WORD: